AUDIT GLASGOW

Comhairle Nan Eilean Siar

Cyber resilience

Final Report

August 2025

Glasgow
CITY COUNCIL

bsi
ISO 9001
Quality
Management
Systems
CERTIFIED

FS 57095

1 Introduction

1.1 As part of the agreed Internal Audit plan, we have carried out a review of the Comhairle's cyber resilience following the cyber-attack which occurred in November 2023.

1.2 The Comhairle suffered a ransomware attack on the 7th of November 2023 which resulted in the encryption and loss of access to data and systems. Currently no Indicators of Compromise (IOCs) have been identified and the root cause of the attack remains unknown. Following the attack and subsequent business continuity efforts, the Comhairle has undertaken several actions to "*build back better*" and improve its security posture.

1.3 An Internal Audit report was published on the 4th of November 2024 which documented the response to the cyber-attack, the lessons learned, and recommendations to reduce the risk of similar incidents.

1.4 The purpose of this audit was to review the actions undertaken by the Comhairle to improve its security posture and IT resilience. The scope of the audit included:

- Reviewing arrangements for log monitoring including the use of a Security Information and Event Management (SIEM) tool and Security Operations Centre (SOC) as appropriate.
- Assessing the current progress regarding the development of a Cyber Incident Response Plan (CIRP) and disaster recovery testing.
- Reviewing the arrangements in place for penetration testing, vulnerability scanning, threat intelligence and the remediation of any issues identified.
- Assessing changes to backup arrangements introduced following the attack.
- Evaluating changes to email security arrangements introduced following the attack.
- Reviewing the patch management procedures and monitoring arrangements in place.
- Assessing the relevant training arrangements for all staff and the IT section.

1.5 Whilst every effort can be made to reduce the risk of a successful cyber-attack, it should be noted that this cannot be eliminated completely. For example, cyber-attacks may seek to exploit zero-day vulnerabilities (a security flaw in software that is unknown to the supplier / vendor for which there are no available patches) or social engineering.

2 Audit Opinion

2.1 Based on the audit work carried out a reasonable level of assurance can be placed upon the control environment. The audit has identified some scope for improvement in the existing arrangements and five recommendations which management should address.

3 Main Findings

3.1 We are pleased to report that the key controls are in place and generally operating effectively. The Comhairle are members of CISP (Cyber Information Sharing Partnership), use the services provided as part of the NCSC's (National Cyber Security Centre) Active Cyber Defence Hub and receive regular vulnerability notifications from SC3 (The Scottish Cyber Coordination Centre).

3.2 External penetration testing is completed on an annual basis as part of the PSN (Public Services Network) IT health check which results in a prioritised remediation action plan. The Comhairle have applied preventative email security controls and “Checkpoint Harmony” has been deployed for email security to help identify and block malicious emails and phishing attempts. Additionally, Sophos MDR (Managed Detection and Response) has been introduced to provide 24-hour monitoring.

3.3 Backup processes have been improved following the attack including a M365 backup solution and monthly backup testing. Information security training and phishing simulation exercises have also been developed and deployed.

3.4 However, our audit testing found that there are some areas which could be improved. The current arrangements for internal vulnerability scanning (other than the annual IT health check) are ad hoc and a documented schedule is not in place. Additionally, incidents that occur out of hours are responded to by IT staff on a best endeavours basis.

3.5 There is not currently a fully air gapped backup, although both on-prem and cloud backups are in place, and we have been advised that discussion are underway regarding implementation of an air gapped backup solution.

3.6 At the time of the fieldwork a cyber incident response plan (CIRP) had been developed. However, this was still to be formally approved and testing arrangements are not yet in place. We have been advised that since the audit fieldwork successful disaster recovery tests have been undertaken.

3.7 While appropriate information security training has been developed for all staff, the completion rate of this is not currently being formally monitored and the schedule for refreshing training has not been defined. Additionally, we have been advised that there is not currently a budget for training of the IT team and a skills assessment of the team is not planed. However, funding has been obtained from Skills Development Scotland to provide training to the IT team.

3.8 An action plan is provided at section four outlining our observations, risks, and recommendations. We have made five recommendations for improvement. The priority of each recommendation is:

Priority	Definition	Total
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	1
Medium	Less critically important controls absent, not being operated as designed or could be improved.	4
Low	Lower-level controls absent, not being operated as designed or could be improved.	0
Service Improvement	Opportunities for business improvement and/or efficiencies have been identified.	0

3.9 The audit has been undertaken in accordance with the Public Sector Internal Audit Standards.

3.10 We would like to thank officers involved in this audit for their cooperation and assistance.

3.11 It is recommended that the Chief Internal Auditor submits a further report to Committee on the implementation of the actions contained in the attached Action Plan.

4 Action Plan

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Vulnerability scans of the IT estate are undertaken regularly.				
1	External penetration testing is completed on an annual basis as part of the PSN (Public Services Network) IT health check and a prioritised remediation action plan produced. However, the current arrangements for further vulnerability scanning are ad hoc and a documented schedule is not in place. We also noted that it is not formally documented when critical patches should be applied out with the planned patch management schedule. Without regular vulnerability scanning and remediation, there is an increased risk that vulnerabilities are not identified and addressed in a timely manner.	Management should review the process in place for internal vulnerability scanning to ensure routine scans are formulised and undertaken in line with the defined frequency. Vulnerabilities identified from the internal vulnerability scanning should be logged and prioritised. The prioritised actions should then be monitored and assigned to a responsible officer to ensure these are mitigated and remediated where appropriate. Management should consider formally documenting when to apply critical patches released out with the planned patch management schedule.	**High**	**Response:** *Since the audit was conducted, a structured patching schedule has been documented and established. This schedule incorporates both routine planned updates and the capability to deploy critical patches on an ad hoc basis, ensuring timely remediation of vulnerabilities.* *Several vulnerability management solutions are currently under evaluation, with implementation anticipated before the end of 2025* **Officer Responsible for Implementation:** *Graham Morrison* **Timescales for Implementation:** *31/12/2025*

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Backups are immutable and air gapped.				
2	Backup processes have been improved following the cyber-attack with on-premises and cloud immutable backup solutions and monthly backup recovery testing. However, a fully air gapped backup is not currently maintained. This would provide a backup which is isolated from the Comhairle's network. Without air gapped backups there is an increased risk that backups could be made unavailable following a cyber incident.	Management should introduce arrangements to maintain a backup that is physically and logically segregated from the Comhairle's network which could be used to aid recovery in the event of a ransomware attack.	**Medium**	**Response:** *Significant industry standard improvements have already been put in place with immutable backups on prem and in the cloud.* *A request for additional funding has been submitted to support the procurement of a fully air-gapped backup solution. Once implemented, this solution will be the third distinct and independent source of data backup, significantly enhancing resilience and recovery capabilities.* **Officer Responsible for Implementation:** *Malcolm Nicol* **Timescales for Implementation:** *Decision on funding by 15/09/2025. Implementation by 31st January 2026*

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: The cyber incident response plan is routinely tested and refined based on the outputs of the testing.				
3	At the time of the audit fieldwork a cyber incident response plan (CIRP) had been developed. However, this was still to be formally approved, and testing arrangements are still to be put in place. If the Comhairle's cyber incident response plan is not tested there is an increased risk that gaps in the plan are not identified before a live cyber incident occurs.	Testing arrangements of the Comhairle's cyber incident response should be developed and approved. Following this, appropriate exercises should be undertaken with the lessons learned used to update the CIRP where appropriate.	**Medium**	**Response:** *Significant successful DR testing has now been carried out, including, Loss of Internet connection, Loss of HQ Firewall and Loss of Virtual infrastructure in HQ.* *Specific CIRP tabletop testing still to be conducted.* **Officer Responsible for Implementation:** *Graham Morrison* **Timescales for Implementation:** *31/12/2025*

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Staff are adequately trained regarding their cyber and information security responsibilities.				
4	While appropriate information security training has been developed for staff, the completion rate of this is not currently being formally monitored and the schedule for refreshing training has not been defined and agreed. We have been advised that there is not currently a budget for training of the IT team and a skills assessment of the team is not planed. If staff have not received appropriate training, there is an increased risk that they are unable to respond to a cyber incident.	Management should formally monitor compliance with the mandatory information security training and where necessary take action to ensure employees undertake the required training. Management should consider introducing a schedule for staff to refresh their information security training. Management should undertake an assessment of training requirements within the IT team to ensure that they are appropriately trained to manage cyber incidents and that there is sufficient breadth of knowledge to cover periods of absence.	**Medium**	**Response:** *Cyber-security training was rolled out as a mandatory course in April 2025. Compliance with mandatory security training is monitored and reported to CMT- compliance is currently around 67%. An email was sent to all Chief Officers in July 2025 detailing completion rates within their service to encourage full compliance. The Comhairle is currently considering the schedule for refresh training.* **Officer Responsible for Implementation:** *Scott McConnell (Training Officer)* **Timescales for Implementation:** *31/12/2025*

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: The Organisation responds in a timely and effective manner to cyber incidents and alerts.				
5	Cyber incidents and alerts that occur out of hours are currently responded to by IT staff on a best endeavours basis. If there are not formal arrangements for responding to cyber incidents out of hours, there is an increased risk that there is a delay in undertaking actions which could contain the event.	Management should consider formalising the arrangements in place for staff who are required to respond to immediate cyber threats that occur out of hours. This should consider the availability of essential staff, procedures and responsibilities.	**Medium**	**Response:** *Currently there are no formal arrangements for out of hours support however staff are compensated should they have to deal with an incident. Formal arrangements will be put in place with a department restructuring that is being conducted by the Head of Service.* **Officer Responsible for Implementation:** *Calum Mackenzie* **Timescales for Implementation:** *31/07/2026*